



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

KRISHNA *et al.*

Application No.: 09/610,798

Filed: July 6, 2000

For: **Distributed Processing in a
Cryptography Acceleration Chip**

Confirmation No.: 4877

Art Unit: 2164

Examiner: Ortiz, Belix M.

Atty. Docket: 1875.4310003

Arguments to Accompany the Pre-Appeal Brief Request for Review

Mail Stop: AF

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby submit the following Arguments, in five (5) or less total pages, as attachment to the Pre-Appeal Brief Request for Review Form (PTO/SB/33). A Notice of Appeal is concurrently filed.

Arguments

Applicants' arguments in the Amendment and Reply under 37 C.F.R. §1.111 filed on August 25, 2006 (hereinafter "Reply"), were not properly considered or responded to by the Examiner in the final Office Action mailed November 13, 2006 (hereinafter the "Office Action"). In the Office Action, the sole independent claim, claim 24, was rejected under 35 U.S.C. §103(a) as being unpatentable over Leung, U.S. Patent No. 6,760,444 (Leung), in view of Gunter, et al, U.S. Patent No. 6,751,728 (Gunter), and further in view of Chang, et al, U.S. Patent No. 6,862,278 (Chang). The Examiner's response was legally and factually deficient because the Examiner failed to show that the cited references taught or suggested a device including "a distributor unit in the device that distributes a plurality of packets and security association information associated with the plurality of packets according to a distribution scheme" and/or "a plurality of security

processing engines in the device, coupled to the distributor unit, that perform authentication and cryptographic functions, wherein the plurality of security processing engines receive at least a portion of the security association information associated with the packets, and wherein the plurality of security processing engines process the plurality of packets in parallel," as recited in the independent claim 24. The Examiner's response was further legally and factually deficient because the Examiner failed to show that a suggestion or motivation to combine the references exists.

1. "A Plurality of Security Processing Engines ... Wherein the Plurality of Security Processing Engines Process the Plurality of Packets in Parallel"

In the Office Action, the Examiner acknowledges that "Leung does not teach a plurality of security processing engines in the device, coupled to the distributor unit, that perform authentication and cryptographic functions." (Office Action, p. 3). The Examiner has taken the position that Gunter teaches this limitation. In Response to Applicant's Reply, the Examiner asserts that Gunter, et al "teaches cryptographic engines on figures 3, 5, and 8; And 'when the receiving host receives the modified packet, it decrypts the encrypted portion and authenticates the packet by calculating another hash value based on the addresses and data in the received packet, and comparing this hash value with the hash value included in the packet' (see Gunter et al., column 2, lines 1-9)." (Office Action, p. 10). Neither the figures or the cited text support the assertion that Gunter teaches "a plurality of security processing engines in the device."

Figure 3 of Gunter simply shows an encrypted packet being transmitted to a network access point (NAP) 70. Figure 3 does not illustrate the structure of a NAP 70 or any network entity (e.g., receiving host 66 or sending host 62). Figure 5 of Gunter is a diagram of a data structure 120 from which a packet is constructed. The data structure

120 illustrates that data 112 and cryptographic hash 116 of data structure 120 are encrypted. Figure 8 of Gunter and the text cited by the Examiner both describe that after a receiving host receives a packet, the host first decrypts the packet and then authenticates it. (Gunter, col. 8, lines 64-65). Despite the Examiner's assertions, nowhere does Gunter teach or suggest that the receiving host includes a plurality of security processing engines. Furthermore, the processing described by Gunter occurs sequentially. Thus, nowhere does Gunter teach or suggest "wherein the plurality of security processing engines process the plurality of packets in parallel," as recited in independent claim 24.

Chang does not overcome these deficiencies of Leung and Gunter. Chang describes a "system and method for parallel compression and decompression of a bit stream." (Chang, Abstract). In the Office Action, the Examiner appears to be equating the parallel compression by multiple encode units and decompression of a bit stream by multiple decode units to the parallel processing of a plurality of packets by the security processing engines in Applicants' claim 24. Chang does not teach or suggest that the encode units and decode units perform any type of security or cryptographic function. The words cryptography, encryption, decryption, or security are not even used in Chang.

2. "A Distributor Unit"

Claim 24 recites, among other elements "a distributor unit that distributes a plurality of packets and security association information associated with the plurality of packets according to a distribution scheme." In the Office Action, the Examiner asserts that Leung teaches a device including a distributor unit citing to Figure 1, col. 2, line 57 - col. 3, line 15 ("Leung passage 1"), and column 7, lines 33-50 ("Leung passage 2"). Figure 1 of Leung illustrates a Mobile IP network segment and does not include

structural details of the illustrated network elements. Leung passage 1 generally describes a registration request packet and a registration reply packet. Leung passage 2 describes that a server receives a packet from a home agent, obtains a security association for the mobile node identified in the packet, and sends a packet, including the security association, in the appropriate format to the home agent. Thus, Figure 1 and Leung passages 1 and 2 simply describe a reply to a received message. Nowhere does Leung teach or suggest "a distributor unit that distributes a plurality of packets and security association information associated with the plurality of packets according to a distribution scheme," as recited in independent claim 24. This deficiency of Leung is not in any way remedied by Gunter or Chang.

3. *No Suggestion or Motivation to Combine Leung, Gunter, and Chang Exists*

"[T]here must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the reference teachings." MPEP §2142. "The motivation, suggestion or teaching may come explicitly from statements in the prior art, the knowledge of one of ordinary skill in the art, or, in some cases the nature of the problem to be solved." *In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999).

The explicit statements referenced by the Examiner in the office action do not provide a motivation or suggest to combine Leung and Gunter or Leung and Chang. (See Office Action, pp. 3-4). Furthermore, the nature of problems to be solved by each of the cited references in the combination are diverse and unrelated. Leung is directed to methods and apparatus for authenticating a mobile node where a centralized database stores security-associations for mobile nodes supported by multiple Home Agents and performs Mobile IP authentication of these mobile nodes. (Leung, col. 4, lines 57-62).

Gunter is directed to the efficient transmission of encrypted packets between a sending host on an external network and a receiving host on an intranet through a network access point (NAP) of the intranet. (Gunter, col. 2, lines 25-40). Chang is not in the field of cryptography and is not reasonably pertinent to the problem of accelerating cryptographic operations with which Applicants were concerned. (See Applicants' specification, p. 5, lines 14-16). Chang, in contrast, is directed to the parallel compression and decompression of a bitstream. (Chang, Abstract). Leung and Chang and Gunter and Chang are simply nonanalogous and as a result are directed to solving completely different problems.

Based on the above, Applicants respectfully request that the rejection of independent claim 24 as obvious be reconsidered and withdrawn. The deficiencies of Leung, Chang, and Gunter with respect to independent claim 24 are not in any way remedied by Barlow, Robinson, and/or Martin. Accordingly, Applicants respectfully request the rejection of dependent claims 25-41 be withdrawn as well.

The U.S. Patent and Trademark Office is hereby authorized to charge any fee deficiency, or credit any overpayment, to our Deposit Account No. 19-0036.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.



Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: March 13, 2003

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600